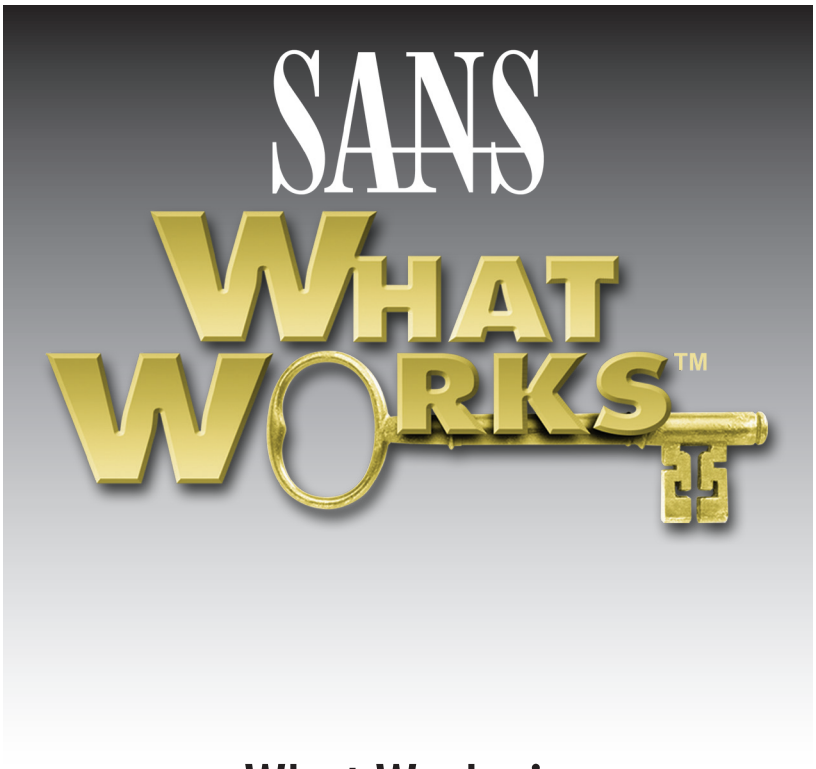

What Works in Visibility, Access Control and IOT Security – Pulse Secure NAC Outcomes at Energy Provider

SPONSORED BY

WhatWorks is a user-to-user program in which security managers who have implemented effective Internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned. Got a story of your own? A product you'd like to know about? Let us know.

www.sans.org/whatworks

ABOUT ENTEGRUS

A medium-sized Canadian power company that has facilities and users spread across multiple regions, with a wide mix of IT and OT devices connecting to many different networks. By integrating Pulse Secure Network Access Control to their network fabric, they were able to gain visibility into the assets in use, as well as enforce access controls while minimizing any business-user disruption. They leveraged their existing Pulse Secure VPN implementation to expedite NAC deployment and fortify their infrastructure in accordance with NIST, NERC and other compliance guidelines. As a result, their security organization extended visibility for remote and on-premise users and devices, as well as enhanced endpoint compliance and Internet of Things (IoT) risk mitigation.

ABOUT THE USER

Dave Cullen is the Manager of Information Technology at Entegrus, a utility company serving 60,000 customers in Canada's southwestern Ontario region. He is responsible for leading IT operations as well as managing the data centre operations for Entegrus Services. His 22 years of IT expertise and certification in Certified Information Systems Security Professional (CISSP), provides strong technical background in managing cyber security and actively participates in Ontario utility industry's IT initiatives.

ABOUT THE INTERVIEWER

John Pescatore, Director of Emerging Security Trends, SANS Institute

John Pescatore joined SANS as director of emerging security trends in January 2013 after more than 13 years as lead security analyst for Gartner, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and voice systems "and the occasional ballistic armor installation." John has testified before Congress about cyber security, was named one of the 15 most-influential people in security in 2008 and remains an NSA-certified cryptologic engineer.

Q Tell us a little bit about yourself and your position at Entegrus.

A My name is Dave Cullen. I am the Manager of Information Technology at Entegrus in Chatham, Ontario. We serve about 60,000 customers across 2400 km² of service territory, delivering electricity, renewable energy and water over three main sites. I manage both the IT and OT infrastructure for the utility company and oversee the small IT team.

Q Since you're the Manager of IT and OT, are you also the CSO, or do you have a chief security person who reports to you?

A No, that would be my hat, as well. I carry CISSP certification; that is one of my primary focuses – our security program here at Entegrus.

Q What was the business issue that drove you to look at solutions where you ended up with technology from Pulse Secure?

A Our business is quite spread out. We have a lot of assets that are across our service territory, perhaps not a high number of assets, but they're in remote locations. We don't have physical visibility on a day-to-day basis on the asset. We have a lot of points where our team members can enter our network, and they need to perform their job; so for us, we needed to employ technology, essentially network access control paired with SSL VPN, in order to gain better visibility and better control of our users and devices access, and be able to provide that ability. We also use NAC to secure specific endpoints on our network that are in remote locations.

Q You mentioned you own both IT and OT. By assets, sounds like you were talking about laptops and maybe fixed PCs. What types of other devices and OT type devices? Was that all part of this?

A For sure we use NAC to identify and enforce policy for devices requesting access or running on our commercial network. However, OT devices typically aren't built with security as a primary focus and there is not the level of access control or monitoring capability within industrial control systems to provide the additional level of security auditing, and protection that we require on the network. We need to employ technologies around those assets to protect them, but also give us the ability and the insight to see what is going on.

Q Since this is often different in the power industry, as part of the commercial network, what end user computing devices do you allow? Do you support BYOD, or is everything company-owned, such as laptops and mobile devices?

A We only allow company-owned devices, and that has been our policy to date, but we are seeing that shift; therefore, we need to be ready to also handle personal devices. While it wasn't a requirement when we made the purchase, BYOD definitely did show up on our scorecard as to what we will have to support because the industry is changing. Our industry is usually a little more static, perhaps a little more cautious to adopt new approaches in technology. But we need to consider that kind of security technology that supports requirements now, and could accommodate what we're going to need to support in the future.

Q As far as the users of the devices, was it all employees, or do you also have third parties that you allow on your internal networks?

A It is both. We do have a high level of vendor support. We do limit their access quite a bit, but we needed technologies that could actually work with their systems, and still allow them to provide the level of support they need to, to us, while, again, maintaining our security standard. That's always a tense relationship in that our security program tends to be more restrictive than perhaps the vendor is used to. We needed a technology that can be flexible, but give us the confidence that they are maintaining our standards.

Q Did you have some key criteria that were top of the list when you started deciding what remote access security and network access control solutions out there you should look at?

A The first thing that we looked at was technical support. What were the support mechanisms available outside of partners and integrators? We focused more on what type of technical support can the manufacturer directly provide? We also look at the openness of the technology, does it have the ability to work with our existing technology stack? In general, what level of interoperability does the technology have? We researched that element, but also wanted to evaluate the functionality in our environment and do some very basic tests with our existing technology stack.

Ease-of-use and the ability to learn the new technology, that was important. We're a small IT team. We don't have the luxury of being able to have a singular focus. We just couldn't dedicate a staff member to be our NAC expert. That's not how things work here. We needed a technology that accommodated our environment and that was easy to learn, but yet was sophisticated enough to meet business demand and meets our security standards.

Q What's your network environment? Are you a Cisco shop, a Juniper shop, a mixed shop, especially related to this project?

A We are predominantly a Juniper shop.

Q How did you go about choosing the best solution? Did you do a paper comparison? Did you do some prototyping, some proof of concept?

A Due to the nature of the technology and our business, we couldn't do what we would normally do, which would be to run it in a full test mode. In this case, we built a lab, and we prototyped in the lab. We brought the potential vendors and narrowed it down by putting each technology through its paces in the lab-really working with the technology. All that while soliciting technical advice, looking at the best practices and ensuring we were following them. Really just looking for how well did everything, operate in the lab and how well it supported our environment.

Q So you did some prototyping and bake-offs in your lab, tested things out, and compared against the initial criteria. What caused you to choose Pulse Secure?

A Pulse Secure, right away, was very easy to integrate into our existing technology stack, not just Juniper, but our Firewall and SIEM, and just it fit right in. I found it to be easy to deploy. We were able to deploy it without interruption and without confusion with our user base. The ability to have both SSL VPN and NAC from the same vendor essentially made it a seamless user experience – that was a definite plus as well. Pulse gave great technical support. We faced hurdles as we were entering new territory, since none of us on the team had ever worked with this type of technology before. With the other products we tested, there were features that we couldn't get working or became more complicated. Pulse gave us the support to make sure everything worked, before we spent money on the technology. I think that was critical, the human element of support. The technology is the technology, but to have that support and to have that expertise there to just say is this the best way should we should attempt this deployment – that was invaluable as we went through and made our decision.

Q How did you go about doing the rollout, the deployment?

A It was a phased approach. We started with Pulse's SSL VPN. We were upgrading from older technology and that was where we had the higher priority initially. We started with that, and we implemented it (Pulse Connect Secure) with Pulse appliances. This included their VPN client on our company-owned devices. Then we moved into NAC (Pulse Policy Secure). We rolled that out in phases, as well.

For NAC, we started with a very basic configuration to obtain network visibility. We then really started to tighten up endpoint security and turn on the advanced functions like enforcement - all with support from Pulse. That allowed us to roll it out over the period of a few months and really gave us a seamless experience for our users. The best technology is a technology that the users don't know is really there. We were able to roll NAC out and limit the impact on users, but also limit the impact on our OT network as well. The OT side of our network does not tolerate change very well. So being able to do it in a phased approach and turn on functionality as we went along, that really contributed to a successful deployment.

Q How did you avoid NAC deployment pitfalls? What sort of policies did you start with and how did you proceed from there?

A We started with a very vanilla configuration. First, we focused on getting the interaction with our switching and our firewalls nailed down. Next was ensuring the Pulse Secure client was operating correctly in every scenario, whether that's SSL VPN, or connections from whichever of our service center networks that employees might be working in, making sure all those interactions were solid and functional. From there we started with host checking functionality and began profiling our device; so it gave us the intelligence and visibility into endpoint security and configuration issues, and we found there were things that we needed to correct, for sure. It gave us visibility that we didn't have before. It showed us

operational trends and gave us some very useful intelligence that we could apply to optimize taking that next step.

From there, we implemented endpoint compliance policies and moved to enforcing elements discovered through host checking, whether it's verifying AV or patching, or other configuration requirements. We created quarantine VLANs. We have a number of policies and respective VLANs based on the device and the identity of the person who is on that device. From that we built dynamic VLAN functionality to really govern the security zone that each individual user with their respective device ends up working from. We made that progression from very vanilla NAC deployment to now being able to dynamically enforce policies based on the health and security state of the device, what device it is, and who the user is on that device - that has been quite valuable in terms of our security posture.

Q Is it really by user, or is it by group or by both?

A We do it by user and the user's role. We are a small organization, so we maybe have some luxuries there. I could do it by group otherwise. It's very easy for us to define policies based on who a person is, what their job function is, and what they should have access to. In a large organization, I would scale that using groups and directories. We really focused on the relationship between the user, who they are, and the device they're using, having that match to be able to drive a scenario. If an admin-level user logs into a device that is never to be used for admin level tasks, we will enforce the lesser privilege. We will assign the device to probably just a standard workstation VLAN, for example. However, if I log into my admin device as an admin user, I will be assigned different rights. We have the luxury, again, of being able to do that because we do have a lower user count, but I could see that translating well to groups, and Pulse makes it easy either way, really.

Q What triggers the NAC process – obtaining an IP address, user authentication, both?

A It starts with the device's request for an IP address, and then we match it with the authentication. The Pulse Secure client plays a major role in that. That way we don't have multiple systems trying to authenticate or re-authenticate, or prompting the user for authentication. The client is installed or can be non-persistent. Important to note, we were able to very easily tie in our multifactor authentication, which is Duo Security. That was very easy to integrate for where that's required as Pulse uses open standards and works with many security vendors. At a device request, it is sitting on the quarantine VLAN, and then we graduate it once those authentication elements are established and policy has been satisfied.

Q One thing everybody runs into in NAC is non-user devices, such as, wireless printers, print servers, or VoIP phones and things like that. How does your Pulse Secure NAC implementation handle those?

A At some point we do have to have to rely on the MAC Address, obviously, and so we do have some of that where we are simply looking at MAC Address filtering. We ensure that those type of devices have very minimal privileges. Our NAC combines addition context (e.g. SNMP, NMAP and DHCP) with MAC Address to further classify a device. Being able to do dynamic VLAN assignment integrated with our switching and firewall infrastructure really allowed us to do a lot of micro-segmentation. I know that's not specific to NAC, but the ability for Pulse Secure to deliver that support for the level of micro-segmentation has proven quite strong.

Q When did you get started? How long have you been using Pulse Secure?

A Following our SSL-VPN upgrade to Pulse Secure, our NAC went into that first phase in September 2016, and we have been successfully running it for 18 months.

Q Who administers the NAC system – did you need to create a dedicated admin staff?

A We were able to blend in with our existing network and security staff, and really support it with our existing headcount. That was great news. We have it in sort of an amalgamated practice, like where we integrate it with other monitoring systems, and other pieces of our security infrastructure. This lets us do a lot of the monitoring of all this infrastructure from one central pane of glass. The ability of the Pulse technology to integrate with other systems is quite good, and it truly is open.

Pulse Secure does support working with network and security infrastructure, and that's been critical because, again, we have a small IT team. We don't have the ability to put teams

of people on individual systems and silo our systems. Another point I would make is we recently went through a merger. We had team members join from that organization, and their experience with remote access was Microsoft. Even so, with Pulse SSL VPN and NAC, they've been able to hit the ground running in helping us support Pulse and support the merged user and device base. It's been a quick and seamless process to get new staff up to speed from an administration perspective.

Q You mentioned one of your important criteria was the techincal support. In the 18 months or so how has the support been from Pulse Secure?

A It's really good. And it's great that I can go get support that extends beyond fixing the problem I'm presently having. NAC is not easy if you're new to it. There are multiple ways to accomplish what you're trying to do. For us, having that technical resources to help us with best practices has been quite good. And it's localized, too, so Canadian-based customer support has been great.

Q Did you see any benefits from using VPN and NAC from the same vendor?

A We initially had Juniper's VPN. So there was benefit of going it with a company we knew. Albeit we started with Juniper and I would say Pulse has differentiated the VPN quite quickly and effectively. That aside, we see the benefits in having those systems work in concert. We brought the user, device and compliance policies from the VPN right into the NAC. And they use the same endpoint client. And we can manage both from the same console. This reduced the complexity and we can maintain the security policies, by virtue of NAC and SSL VPN working together, while having a seamless and easy experience for our end users.

Q So based on what you know now, are there any lessons learned you can pass on or have done differently when you got started; if you knew what you know now?

A I would have done NAC sooner. It's not ultimate security, but it is a fundamental piece that improves your security posture quite quickly. It can be a difficult technology to integrate, though. You need to have a good grasp of your infrastructure. We waited too long to do it. We could have improved our security posture much more quickly if we had done it sooner. I think we did a good job of focusing on the user experience. I think that's crucial and was reaffirmed in the process that if you try and go full bore and you implement NAC too quickly or you don't take a detailed look at the experience for the user, you're going to run into support nightmares. To a large extent that is just the nature of the technology. It will block bad things from happening, and if you understand the user's needs, you can determine where and when to enforce policyminimize to disruption to legitimate business actions. So, I believe a good take-away is have an innate focus on the end-user experience. Have a very good grasp of the layout of your networks and devices that are on it, and expect some things to break. It wasn't our users' ability to work, but we did have devices on the network that did not work when we turned NAC on. Be able to plan for that and create a buffer.

Q What are your plans for the future with the Secure Access technology and Pulse Secure products?

A Certainly there have been a few updates since we originally deployed, and we want to start looking more at the enterprise on-boarding and integration features. We also want to see what more we can do with the profiling data and for other systems. We're gathering a lot of good data on a device starting from its first touch to the network. What can we do with that data? Pulse Secure NAC visibility and enforcement capabilities have been great, and we're confident that it will secure and assign resources based on our profiles and policies. But what can we do with that data to help us make better decisions? What new policies should be implemented, what micro-segmentation structure we should have in our network? How do we enhance that? Ultimately, how do we make sure that we're running the most efficient, and protected network possible? We want to start using that data that we're generating even, deeper.